HIPAA&TRICARE

March 2003, No. 5

Newsletter

Health Insurance Portability and Accountability Act

Inside This Issue . .

Final Security Rule is Published

The final HIPAA security rule, which was released for comment as a Notice of Proposed Rule Making (NPRM) in August 1998, was published in the Federal Register on February 20, 2003. While the final rule becomes effective April 21, 2003, most covered entities will have until April 21, 2005 to comply with the standard. Small health plans will have an additional year to meet compliance (April 21, 2006). The security rule was created in an effort to protect the confidentiality, integrity, and availability of a patient's protected health information (PHI) by adopting national standards for PHI that is created, received, maintained or transmitted electronically.

> ***"The security final rule clearly defines a realistic model for security management"***

Whereas the draft rule focused on the specifics of technology implementation, the final rule emphasizes security management principles and broad management controls as the primary means of protecting electronic health information. Significant changes highlighted in the final rule are:

- Removal of information pertaining to electronic signature standards (electronic signature standards will be published in a separate final rule);
- Modification of several implementation features so they are now "addressable" rather than "mandatory;" and
- Combination of Technical Security Services and Technical Security Mechanisms to be referred to as "Technical Safeguards."

The standards of the final security rule work in concert with the final privacy standards adopted by the Department of Health and Human Services (HHS) last year. It is important to recognize the difference between security and privacy, as the security standards define administrative, physical and technical safeguards to protect electronic health information. The privacy rule, on the other hand, sets standards for how PHI should be controlled, by determining what uses and disclosures of that information are authorized and what rights patients have regarding their health information. Another distinction that should be highlighted is that the privacy rule applies to PHI in any form whereas the security rule applies only to PHI in electronic form.

Before the security rule, no standard measures existed in the health care industry that addressed all aspects of the security of electronic health information. The HIPAA final security rule will enforce security of health information and is broken into three categories: Administrative Safeguards, Physical Safeguards, and Technical Safeguards. Administrative Safeguards contain several standards that address the business policies and processes that allow access to and protection of individually identifiable health information that is in electronic form. Some of the standards in this section include security management, workforce security, information access management, and security awareness and training. Physical Safeguards focus on the Military Treatment Facility (MTF) as a physical facility and the physical security mechanisms including facility access controls, device and media controls, and workstation security. The Technical Safeguards section of the final rule contains standards that deal with technical policies and procedures for electronic information systems.

The final security rule clearly defines a realistic model for security management that is broadly flexible across the healthcare industry. The Department of Defense (DoD) Security Working Integrated Project Team (WIPT), with representatives from all three Services, is currently working to develop implementation strategies for MTFs and Military Health System (MHS) personnel. ■

MTF Privacy Officer Action Plan

With the HIPAA privacy rule compliance date, April 14, 2003, just around the corner, it is important that all Military Treatment Facilities (MTFs) be prepared to meet this requirement. The following information serves as an action plan for each MTF and MTF Privacy Officer, and outlines which actions should be complete, occurring presently, or remain to be achieved by April 14, 2003.

The privacy rule requires each covered entity, including medical and dental treatment facilities (DTFs), to appoint a Privacy Officer who is responsible for overseeing all ongoing activities related to the development, implementation, and maintenance of the MTF/DTF policies and procedures covering the access to and privacy of patient health information. At this time, each MTF/DTF should have a Privacy Officer and he or she should have briefed the MTF Leadership on the implications of the privacy rule. Additionally, the MTF Action Plan should be completed as well as the identification of all relevant MTF policies and procedures.

It is imperative that each MTF Privacy Officer keep abreast of what is expected of their MTF to be in compliance with the privacy rule. To be compliant by April 14, 2003, MTFs and MTF Privacy Officers must provide Privacy Awareness Training for all MTF staff as well as provide the level 200 courses to all appropriate staff. All training that has occurred *must* be documented. Privacy Officers should also develop local policies and procedures to protect health information at MTFs and other offices by utilizing the Compliance Tool made available by TRICARE Management Activity (TMA). Both tools can be found at: http://www.tricare.osd.mil/hipaa/Training-and-Compliance.htm.

TMA strives to have all Military Health System MTFs in compliance with the privacy rule, by the April 14th compliance date. TMA has made an effort to ensure this result by providing the tools and training necessary to achieve privacy compliance. The job of the MTF Privacy Officers does not end once the MTF meets compliance. Instead they are responsible for continuing to understand and conform with Service level reporting requirements as well as tracking HIPAA developments via the TMA/HIPAA Website. ■

Time Frame	Actions
Completed	Brief MTF Leadership Development of Action Plan Identify all relevant policies/procedures Provide interim Privacy Awareness Training
Now	Document Privacy Awareness Training Begin to develop local policies/procedures
April 14, 2003	Provide Privacy Awareness Training for all staff Provide Level 200 courses to appropriate staff Document all training Perform compliance assessments using Tool Complete policy and procedures implementation
On-Going	Understand and conform with Service level reporting requirements Track HIPAA developments via TMA HIPAA Website